by Schneider Electric

INSTALLATION

DX8100 Series Important Security Information

System Administrators

C2641M-C (7/09)

Contents

DX8100 Platform Security Information 5
Physical Security 5
Setting the BIOS Supervisor Password 6
Operating System Security 9
Windows Operating System Updates 9
Changing the Administrator Password 9
Enabling Automatic Logon 12
Enabling Ctrl+Alt+Del 13
Using F2+F9+Del 13
DX8100 Security 14
Internet Protocol Security 14
Firewalls 14
System Management 14
DX8100 Network Ports 15
Application Software 15
Password Recovery 16
Starting the DX8100 Server in Safe Mode 17

List of Illustrations

1 DX8100 BIOS Setup Main Screen 6
2 New BIOS Password Dialog Box 7
3 Password Confirm Dialog Box 7
4 BIOS Setup Confirmation Screen 8
5 Users and Passwords Icon in Control Pane 9
6 User Accounts Dialog Box 10
7 Changing Your Account Prompt 10
8 Change Your Passwords Dialog Box 11
9 Log On to Windows Dialog Box 11
10 User Accounts Dialog Box 12
11 Automatically Log On Dialog Box 12
12 DX8100 IPSec Policy Dialog Box 14
13 Password Recovery Option in File Menu 16
14 Password Recovery Dialog Box 16
15 Boot Agent Window 17
16 Windows Advanced Options Menu Window 17
17 Please Selecting the Operating System to Start Window 18
18 Desktop Dialog Box 18

List of Tables

A Keyboard Remapping 13
B Open Ports on the DX8100 15

DX8100 Platform Security Information

The DX8000 Series hybrid video recorder (HVR) is equipped with an extensive set of security measures to provide the user with secure, uninterrupted service.

NOTES:

- While great care has been taken in the design and development of the DX8100 to ensure a secure HVR platform, it is not feasible to protect a system from all internal and external security risks if it is connected to an unsecured network. In addition to the robust security features built into the DX8100, you should consult with your network administrator, information technology department, and facilities manager to ensure that all possible measures are being taken to ensure the safety and security of the DX8100 and its data.
- For information about upgrading or reinstalling DX8100 software, refer to the DX8100 Upgrade and Recovery manual.

The following sections describe the security features of the DX8100 in detail. These sections are intended for system administrators who are responsible for the maintenance and security of the DX8100.

PHYSICAL SECURITY

Like any other video recording device, including VCRs, the security of the DX8100 is largely dependent on the physical security of the unit itself. When an intruder has access to the hardware, it will be possible to remove components and retrieve recorded data. Units should therefore be installed in a location that is physically secured.

Because the dimensions and underlying technologies of the DX8100 are similar to those of a modern personal computer, it is possible to rack mount units and access the mouse and keyboard inputs using commercially available keyboard video mouse (KVM) switches. This may bring the control of the units outside of the secured area. One area where this could cause a problem involves access to the system's basic input/output system (BIOS). Pelco recommends that the unit be given a BIOS supervisor password upon completion of installation. A unique BIOS supervisor password will help prevent remote operators from changing boot parameters that could allow the unit to be booted using unsecured sources.

The DX8100 is engineered to reboot automatically in the event of a system problem. The capability of recovering from certain errors without operator intervention minimizes the potential amount of time an HVR will be offline. To retain this capability, it is important that a password be set for BIOS Supervisor account only and not for the BIOS User account. Setting a password for the BIOS User account would force operators to re-enter this password each time the system is rebooted.

⚠ **WARNING:** Always scan removable media, such as CD-RW and DVD-RW disks, for viruses before inserting them into the DX8100.

SETTING THE BIOS SUPERVISOR PASSWORD

The following procedure describes how to set the BIOS supervisor password. This procedure should be performed only by advanced users with extensive experience with PC computer technology. Changing BIOS settings to incorrect values may result in the degradation of system performance or cause your HVR to stop working.

To set the BIOS supervisor password:

1. Boot the DX8100 Series HVR by turning on the power switch.
2. Press the Delete key on the keyboard as soon as the Pelco splash screen is displayed. The BIOS Main screen opens.

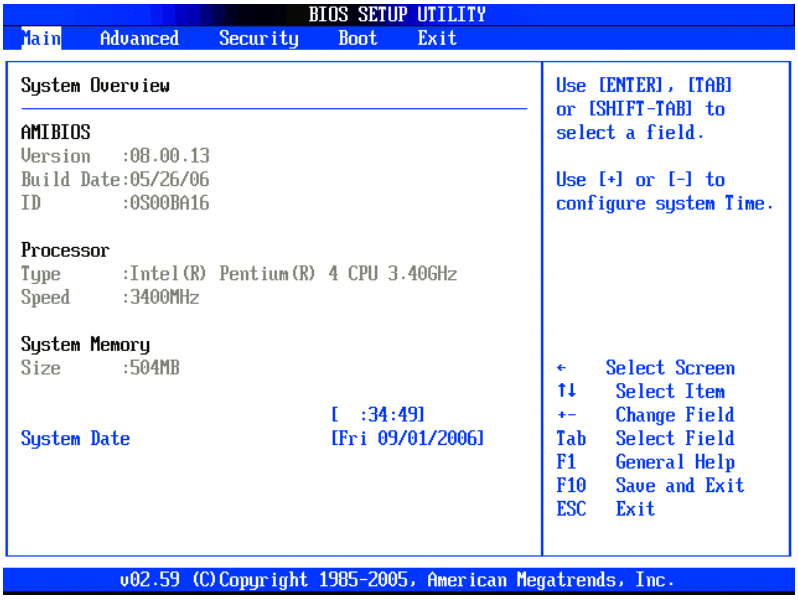

Figure 1. DX8100 BIOS Setup Main Screen

3. Use the cursor control keys on your keyboard to move over to the Security tab and select Change Supervisor Password.
4. Press the Enter key on your keyboard. The Enter New Password dialog box opens.
5. Enter a new password for the BIOS Supervisor account. Passwords should be between four to six alphanumeric characters.

6. Press Enter to accept the new password.

⚠ **WARNING:** Make sure that you only set the BIOS supervisor password. Do not assign a password to the BIOS user password.

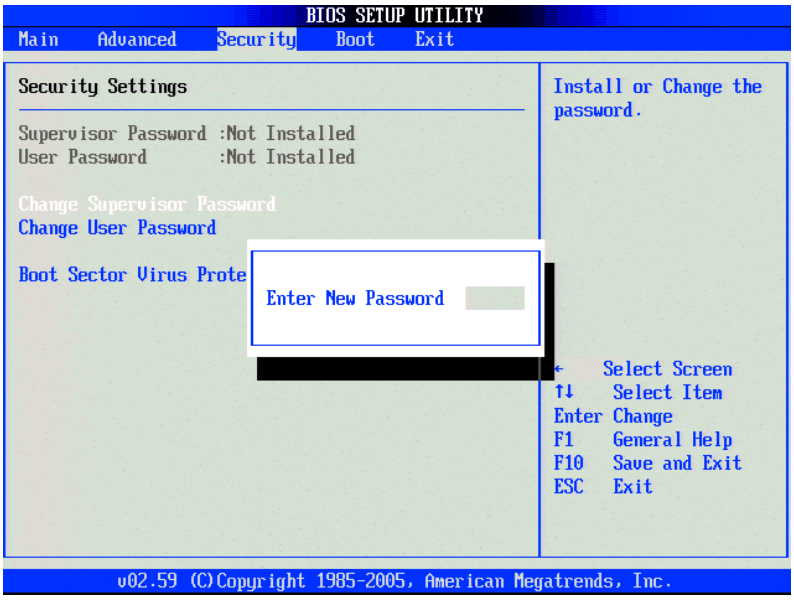

Figure 2. New BIOS Password Dialog Box

7. Re-enter the password to confirm that it is correct.
8. Press Enter to confirm the new password.

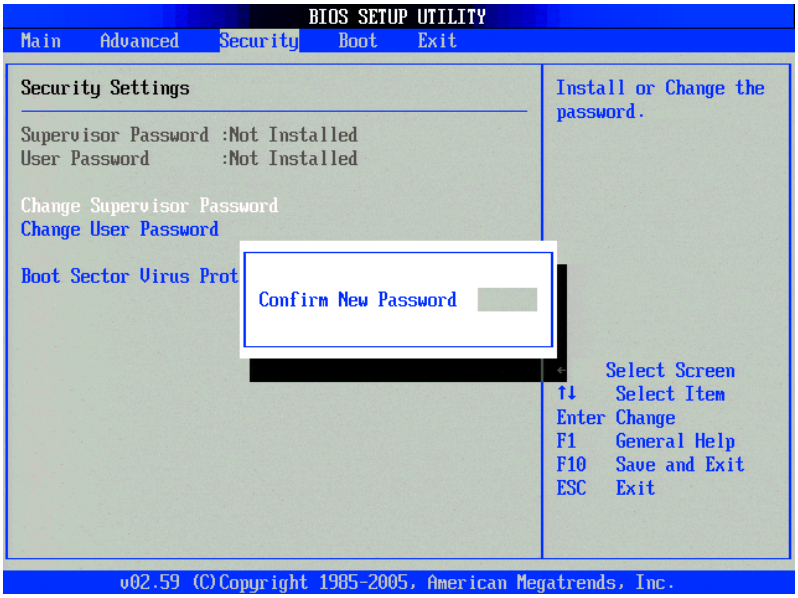

Figure 3. Password Confirm Dialog Box

NOTE: Remember to write down this password and keep it in a secure place.

9. Press the F10 function key on your keyboard to save and exit the BIOS setup screen.

10. Finalize BIOS changes:
    - To accept the BIOS changes and reboot, press the Enter key.
    - To cancel the BIOS changes, press the Esc key and Ctrl+Alt+Delete to reboot the DX8100.

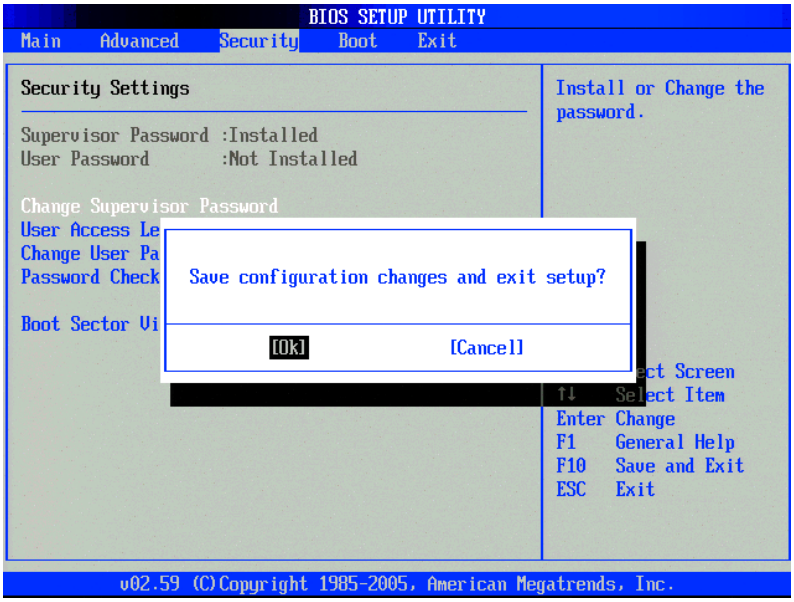

Figure 4. BIOS Setup Confirmation Screen

OPERATING SYSTEM SECURITY

Upon a successful boot procedure, the DX8100 will automatically load the Microsoft® Windows® XP Embedded operating system. These operating systems are specifically tailored for use on the DX8100. It does not have the standard feature set found in the commercially available version of the Windows XP Embedded operating system. This means that services that are not needed for the correct operation of the DX8100 have been removed to eliminate potential vulnerabilities.

Only two user accounts are available in the DX8100's operating system software. These user accounts should not be confused with the accounts assigned by the DX8100 application software. An administrator account allows a designated user to make changes to the registry and security settings to accommodate the requirements of the specific site.

In finding a balance between security and functionality, Pelco has consistently opted for security but leaves it up to the administrator to unlock features that might be useful if the administrator has determined that the additional security of the lockdown is not needed. A typical example of this is the capability of the DX8100 to use dynamic IP addresses. Because IP addresses can change over time, clients must use a different mechanism to connect to the server than by simply providing an IP address. The additional use of NetBIOS protocol services allows the computer to find IP addresses on the local LAN by system name; it should be noted that this also creates a known vulnerability. To allow the end user to use the NetBIOS feature, the services are activated at the factory, but they can be disabled by an administrator when needed. When NetBIOS services are activated, the administrator needs to apply alternative means to protect against hackers and viruses such as a firewall. Please check with your information technology specialist or contact Pelco Product Support for further instructions.

WINDOWS OPERATING SYSTEM UPDATES

Due to the lockdown of nonessential services on the DX8100, administrators are advised against installing every operating system upgrade published by Microsoft. The majority of these updates are not applicable to the DX8100. Pelco will provide a list of approved updates upon request.

CHANGING THE ADMINISTRATOR PASSWORD

To change the Windows XP Embedded DX8100 administrator password:

1. Exit the DX8100 application if it is running, and return to the Windows operating system.
2. Click Start > Settings > Control Panel. The Windows Control Panel opens.

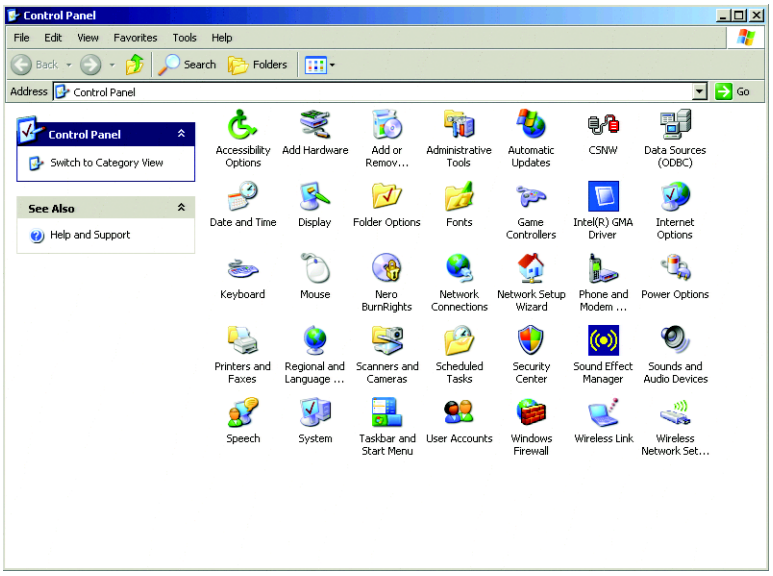

Figure 5. Users and Passwords Icon in Control Pane

3. Double-click the User Accounts icon. The User Accounts dialog box opens.

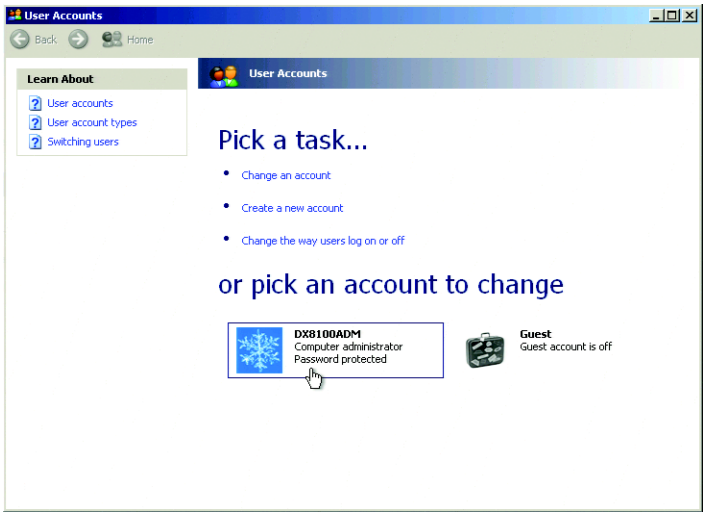

Figure 6. User Accounts Dialog Box

4. In the accounts list, click the DX8100ADM account. The User Accounts dialog box displays "What do you want to change about your account?"

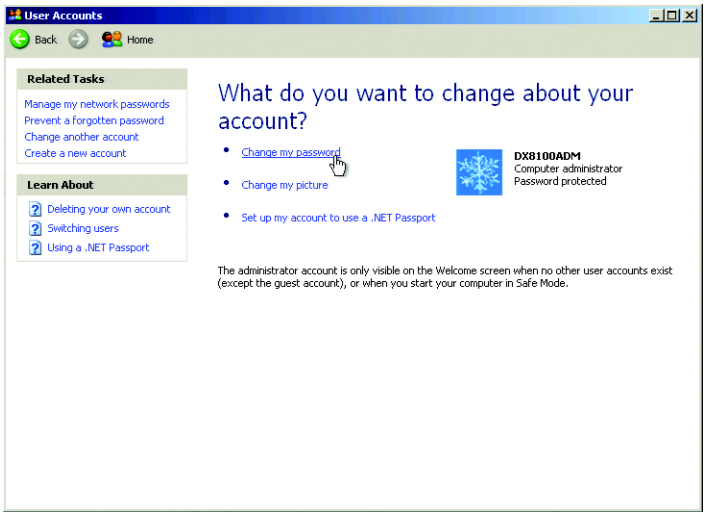
User Accounts
Back
Home
Related Tasks
Manage my network passwords
Prevent a forgotten password
Change another account
Create a new account
Learn About
Deleting your own account
Switching users
Using a .NET Passport
What do you want to change about your account?
Change my password
Change my picture
Set up my account to use a .NET Passport
DX8100ADM
Computer administrator
Password protected
The administrator account is only visible on the Welcome screen when no other user accounts exist (except the guest account), or when you start your computer in Safe Mode.

Figure 7. Changing Your Account Prompt

5. Click “Change my password.” The “Change your password” dialog box opens.

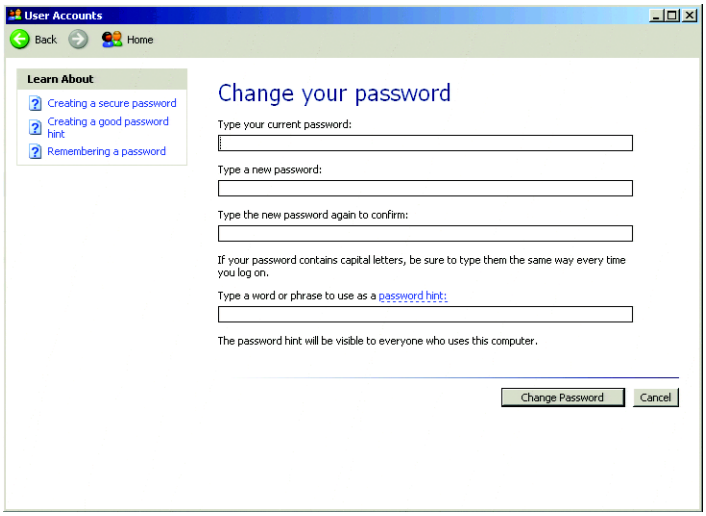
User Accounts
Back
Home
Learn About
Creating a secure password
Creating a good password hint
Remembering a password
Change your password
Type your current password:
Type a new password:
Type the new password again to confirm:
If your password contains capital letters, be sure to type them the same way every time you log on.
Type a word or phrase to use as a password hint:
The password hint will be visible to everyone who uses this computer.
Change Password
Cancel

Figure 8. Change Your Passwords Dialog Box

6. Enter the new password for the DX8100ADM account and then click the Change Password button. A prompt is not displayed advising you that the password is been changed. Instead, the dialog box closes and the User Accounts “Pick a task” dialog box is redisplayed.

   Passwords are case-sensitive and should contain a mixture of alphabetic and numeric characters between six and ten characters in length.

   NOTE: Remember or write down this password and keep it in a secure place.

7. To log on to the DX8100 server application, do one of the following:
   - To manually log on, go to step 8.
   - To enable automatic log on, refer to *Enabling Automatic Logon* on page 12.

8. To manually log on to the server application:
   a. Close the User Accounts dialog box, and then restart the DX8100. The logon message dialog box opens.

   b. Click OK. The Log On to Windows dialog box opens.

Figure 9. Log On to Windows Dialog Box

   c. Enter the new password and then click OK. The DX8100 server application starts.

ENABLING AUTOMATIC LOGON

The DX8100 can be configured to automatically log on to the server. If the password is changed, this feature is disabled. To reactivate the automatic logon feature, you must reconfigure the unit each time the password is changed.

1. To reconfigure the automatic logon, do one of the following:
   - In the Windows environment, go to step 2.
   - In the DX8100 application, exit the DX8100 application, and return to the Windows operating system.
2. To configure the DX8100 to automatically log on to the server application:
   a. On the taskbar, click Start and then click Run. The Run dialog box opens.
   b. In the Open text box, type **control userpasswords2**.
   c. Click OK. The User Accounts dialog box opens.

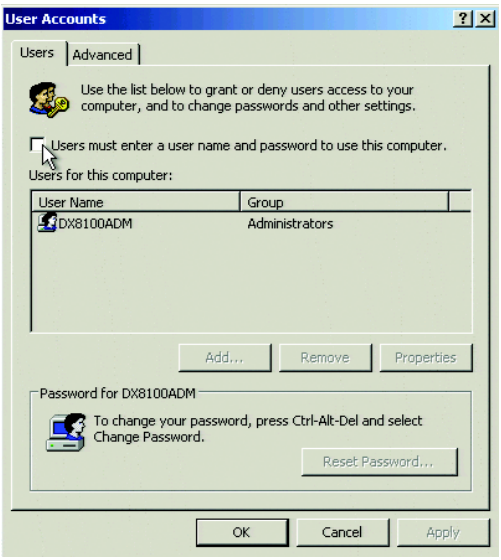

Figure 10. User Accounts Dialog Box

   d. Click the check box "Users must enter a user name and password to use this computer."
   e. Click the check box again to deselect it and then click Apply. The Automatically Log On dialog box opens.

Automatically Log On
You can set up your computer so that users do not have to type a user name and password to log on. To do this, specify a user that will be automatically logged on below:
User name:
DX8100ADM
Password:
Confirm Password:
OK
Cancel

Figure 11. Automatically Log On Dialog Box

   f. In the Password text box, type the new DX8100ADM password.
   g. In the Confirm Password text box, retype the password again.
   h. Click OK and then restart the DX8100 server. The unit will restart and automatically log you on to the DX8100 server application.

ENABLING CTRL+ALT+DEL

Enabling the Ctrl+Alt+Del key combination allows you to open the Windows Task Manager dialog box to perform Windows system administration tasks. To complete the procedure, you must be logged on to the DX8100 application as the Admin user. The standard Ctrl and Alt keys are remapped for the DX8100 application, refer to Table A. The key combination used to implement Ctrl+Alt+Del is F2+F9+Del.

Table A. Keyboard Remapping

DX8100 Key	Windows Action
F2	Ctrl
F4	Space
F9	Alt
Ctrl	Space
Alt	Space

To enable the Ctrl+Alt+Del key feature:

1. Click the Setup button .
2. Click the System button .
3. From the Setup Ctrl+Alt+Del key combination area, click the Enable Ctrl+Alt+Del key combination selection check box.
4. Click Apply.
5. Reboot the DX8100.

USING F2+F9+DEL

The Ctrl+Alt+Del feature must first be enabled. F2+F9+Del allows you to access the Windows Task Manager dialog box from within the DX8100 shell. When you exit the Windows environment, you are returned to the DX8100 shell. In this case, you do not have to log on to the unit again.

To access the Windows Task Manager dialog box:

1. Press F2+F9+Del. The Windows Security dialog box opens.
2. In the Windows Security dialog box, click Task Manager. The Windows Task Manager window opens.
3. To return to the DX8100 shell without rebooting the DX8100, exit the Windows Task Manager dialog box.

DX8100 SECURITY

INTERNET PROTOCOL SECURITY

The DX8100 features built-in network security using Internet Protocol Security (IPSec). IPSec facilitates authentication and encryption at the network packet level. IPSec services protect the DX8100 from unwanted or potentially damaging network requests. With IPSec enabled, the DX8100 HVR will not respond to any unsecured communication across the network, whether friendly or malicious. IPSec only blocks unwanted or unauthorized communication flowing to the DX8100. It does not hinder communication sessions that are initiated by the DVR.

IPSec is enabled by default on the DX8100; however a system administrator can disable the service if it is deemed necessary for the proper functioning of the unit.

⚠ **WARNING:** Disabling IPSec services will expose your DX8100 Series HVR to potentially damaging network traffic. It is highly recommended that IPSec is enabled at all times for the protection of your system.

To disable IPSec services on the DX8100 Series HVR:

1. Exit the DX8100 application if it is running, and return to the Windows operating system.
2. Go to Start > Programs > Manage IPSec Policy. The DX8100 IPSec Policy dialog box opens.

Figure 12. DX8100 IPSec Policy Dialog Box

3. Deselect the Enable DX8100 IPSec Policy check box. Reselect the Enable DX8100 IPSec Policy check box to re-enable IPSec.
4. Click OK.

FIREWALLS

The DX8100 includes the Windows firewall that comes with Service Pack 2 for Windows XP. The security services provided by the Windows Firewall protects the DX8100 from unwanted or potentially damaging network requests. With the Windows Firewall and IPSec enabled, the DX8100 HVR will not respond to any unsecured communication across the network. However, there are potential risks to which you should be aware. The Windows Firewall does not block all ports. For a list of ports required for operation, refer to *DX8100 Network Ports* on page 15.

Pelco recommends that an external network firewall be used. The network firewall will provide additional protection for the DX8100. Regardless of which port or service is under attack, the port must be open or at least visible in order for the malicious program to exploit it. Firewalls filter and render all unneeded ports invisible, providing excellent protection against such attacks. Networked systems exposed in anyway to the outside world (for example, when connected to the Internet) should be equipped with network-based firewall protection.

SYSTEM MANAGEMENT

Any SNMP monitoring software can be used to monitor DX8100 system health events. This section describes the guidelines for implementing DX8100 and SNMP monitoring software communication.

- **SNMP:**
  - Supported versions: SNMPv1 and SNMPv2
  - SNMP community string: pelco
- **NMS:** Although the version 1.2 WinXP firewall is opened to allow incoming SNMP requests on port 161/udp, third-party network management stations (NMS) are not able to query a DX8100 running IPSec.

  To enable a NMS to query the DX8100, select one of the following options:

  - **IPSec on:** Run IPSec on the NMS (with the same passphrase, authentication, and encryption settings) performing SNMP polling.
  - **IPSec off:** Turn IPSec off on the DX8100.

Ping echos are enabled through the WinXP firewall, so that a third-party network management station can auto discover DX8100s (standard procedure).

DX8100 NETWORK PORTS

Table B describes the DX8100 ports and their functions. The ports are classified either as user-changeable or fixed. You can assign a user-changeable port a different number. In this case, a port's number must be assigned within the range of 5000–65535. If a port is assigned out of this range, the system displays a message alerting you that an invalid port number is being used. You cannot assign a different number to a fixed port.

Table B. Open Ports on the DX8100

PORT	User-Changeable	Function
80/tcp	No	HTTP (Hyper Text Transfer Protocol) forms the basis for Web page transfer over the Internet. Ports 1–255 are reserved for well-known services at network communication
135/tcp, udp	No	End Point Mapper (EPMAP), a Microsoft RPC locator service
137/tcp, udp	No	File/print sharing (NetBIOS name service)
1028/tcp	No	Remote Procedure Call (RPC)
1801/tcp	No	Message queuing
1900/udp	No	Universal plug-and-play (UPnP)
2103/tcp	No	Message queuing
2105/tcp	No	Message queuing/logon
2107/tcp	No	Message queuing
2869/tcp	No	UPnP
9002/tcp	Yes	DX8100 base port, used for transmission of video, audio, and interface data
9003/tcp	Yes	DX8100 software upgrade port, used for remote upgrade of DX8100 software
9005/tcp	Yes	DX8100 information port

NOTE: Unless there is a conflict on your network, it is recommended that you do not change port numbers from their default settings. Make sure any changes to port numbers are made consistently across all DX8100 servers and clients on a network.Client and server ports must be identical.

The DX8100 port functionality is summarized as follows:

- **Base port:** This port is configured at the DX8100 Network setup screen. The base port number is downloaded to the PC client system during an IP scan. The port number can be modified at the DX8100 Site setup screen.
- **Software Upgrade Port:** This port is configured at the DX8100 Network setup screen. The upgrade port number is downloaded to the PC client system during an IP scan. The port number can be modified at the DX8100 Site setup screen. The PC client's upgrade port number must match the DX8100 server's upgrade port number. For server-to-server software upgrades, both server software upgrade port numbers must match.
- **Agent Port:** This port is configured at the DX8100 Notification setup screen. You change the client emergency agent server listening port using the Emergency Agent application running on the PC client system. For more information about changing the client emergency agent listen port, see the Client Applications manual.
- **Other reserved ports:** Ports 256–1023 are reserved for well-known services. Ports 1024–4999 are temporal client ports (OS allocates automatically).

APPLICATION SOFTWARE

The only application intended and guaranteed to work on the unit is the DX8100 application software itself. Do not install other application software. If you do, this voids the warranty on the unit, and it also opens up potential holes in the system security. The DX8100 application software has several user and group accounts with varying degrees of rights and permissions on the system. Each account is password-protected. These accounts and passwords are completely different from the operating level account and password discussed in the previous section. The typical system operator will have to work only with application program level user names and passwords.

PASSWORD RECOVERY

There are no “backdoor” accounts or alternative access options built into the DX8100 application software. Pelco cannot issue overriding passwords, factory passwords, or other means to bypass the logon requirement of the application program. If the DX8100´s Admin account password is lost or forgotten, there is only one method for resetting the Admin password without completely reinstalling the system from the Recovery CD.

Upon request, Pelco can issue a unique password recovery code that is valid for 24 hours only. The recovery code is exclusive to the machine for which it is issued. If needed, the original buyer of the system (typically the dealer) may contact Pelco Product Support with the serial number and order or invoice number on which the unit was originally purchased. This must be done in writing, and the request must be accompanied by a letter from the current owner of the system stating the he or she is the legal owner of the system, the password for the system was lost, the MAC address for the HVRs for which a reset code is needed, and that he or she is requesting a password reset code. Upon verification, Pelco will issue a reset code that can be used for 24 hours on the DX8100 with the provided MAC address only.

To recover a lost or forgotten Admin password:

1. Go to File > Password Recovery. The Password recovery dialog box opens.

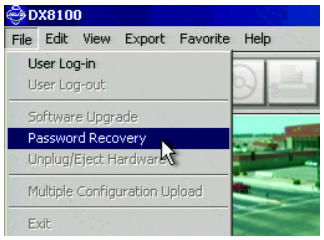

Figure 13. Password Recovery Option in File Menu

2. Contact Pelco Product Support with the following information:
   a. MAC address as it appears in the Password Recovery dialog box.
   b. Current date for your location as it appears in the Password Recovery dialog box.
   c. Any additional information requested by Pelco Product Support

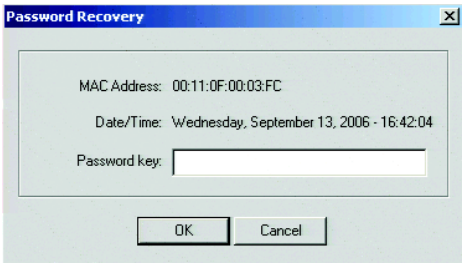

Figure 14. Password Recovery Dialog Box

3. Enter the new password you obtained from Pelco Product Support in the field provided.
4. Click OK.

STARTING THE DX8100 SERVER IN SAFE MODE

DX8100 version 2.0 supports Safe Mode.

1. Restart the DX8100 server. The system displays the message “Exiting DX8100. Please wait...,” and then loads the BIOS (refer to Figure 15).

Figure 15. Boot Agent Window

2. Repeatedly press the F8 function key after the BIOS loads. The Windows Advanced Options Menu window appears.

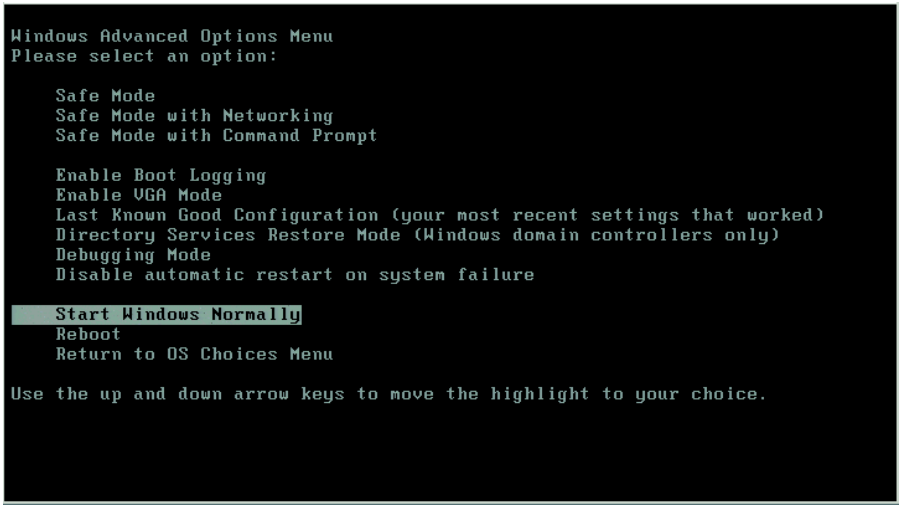
Windows Advanced Options Menu
Please select an option:
Safe Mode
Safe Mode with Networking
Safe Mode with Command Prompt
Enable Boot Logging
Enable VGA Mode
Last Known Good Configuration (your most recent settings that worked)
Directory Services Restore Mode (Windows domain controllers only)
Debugging Mode
Disable automatic restart on system failure
Start Windows Normally
Reboot
Return to OS Choices Menu
Use the up and down arrow keys to move the highlight to your choice.

Figure 16. Windows Advanced Options Menu Window

3. Use the arrow keys to select the Safe Mode option, and then press Enter. The “Please select the operating system to start” window appears.

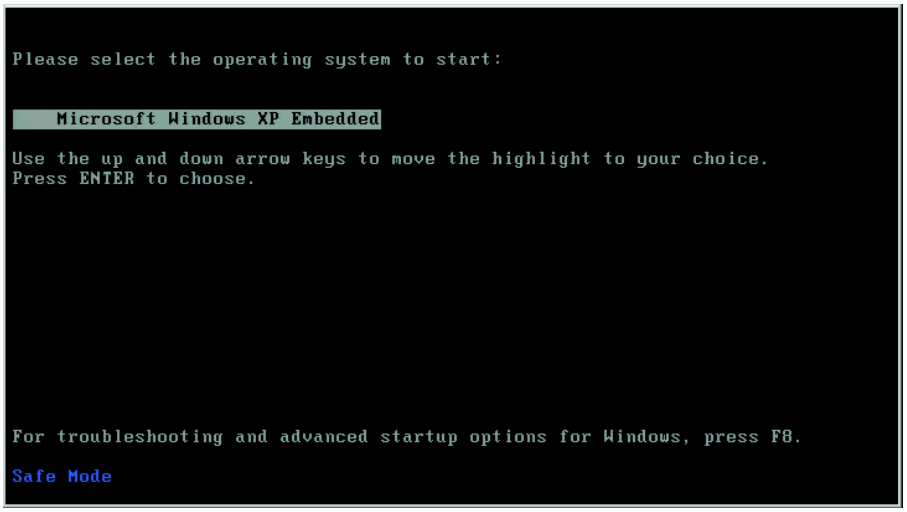
Please select the operating system to start:
Microsoft Windows XP Embedded
Use the up and down arrow keys to move the highlight to your choice.
Press ENTER to choose.
For troubleshooting and advanced startup options for Windows, press F8.
Safe Mode

Figure 17. Please Selecting the Operating System to Start Window

4. If not already highlighted, select Microsoft Windows XP Embedded and then press Enter. The DX8100 error message dialog box appears.
5. Click OK. The Log On to Windows dialog box appears.
6. Enter the Windows password, and then click OK. The Desktop dialog appears.

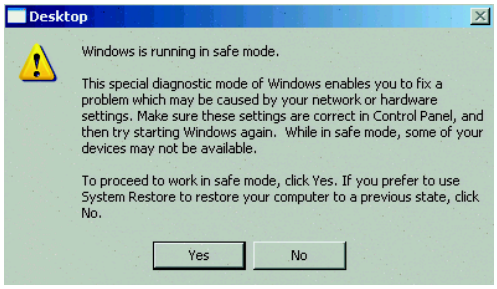
Desktop
Windows is running in safe mode.
This special diagnostic mode of Windows enables you to fix a problem which may be caused by your network or hardware settings. Make sure these settings are correct in Control Panel, and then try starting Windows again. While in safe mode, some of your devices may not be available.
To proceed to work in safe mode, click Yes. If you prefer to use System Restore to restore your computer to a previous state, click No.
Yes
No

Figure 18. Desktop Dialog Box

7. Read the message and click Yes.

PRODUCT WARRANTY AND RETURN INFORMATION

WARRANTY

Pelco will repair or replace, without charge, any merchandise proved defective in material or workmanship **for a period of one year** after the date of shipment.

Exceptions to this warranty are as noted below:

- Five years:
  - Fiber optic products
  - TW3000 Series unshielded twisted pair (UTP) transmission products
  - CC3701H-2, CC3701H-2X, CC3751H-2, CC3651H-2X, MC3651H-2, and MC3651H-2X camera models
- Three years:
  - Pelco-branded fixed camera models (CCC1390H Series, C10DN Series, C10CH Series, IP3701H Series, and IX Series)
  - EH1500 Series enclosures
  - Spectra® IV products (including Spectra IV IP)
  - Camclosure® Series (IS, ICS, IP) integrated camera systems
  - DX Series digital video recorders, DVR5100 Series digital video recorders, Digital Sentry® Series hardware products, DVX Series digital video recorders, and NVR300 Series network video recorders
  - Endura® Series distributed network-based video products
  - Genex® Series products (multiplexers, server, and keyboard)
  - PMCL200/300/400 Series LCD monitors
- Two years:
  - Standard varifocal, fixed focal, and motorized zoom lenses
  - DF5/DF8 Series fixed dome products
  - Legacy® Series integrated positioning systems
  - Spectra III™, Spectra Mini, Spectra Mini IP, Esprit®, ExSite®, and PS20 scanners, including when used in continuous motion applications.
  - Esprit Ti and TI2500 Series thermal imaging products
  - Esprit and WW5700 Series window wiper (excluding wiper blades).
  - CM6700/CM6800/CM9700 Series matrix
  - Digital Light Processing (DLP®) displays (except lamp and color wheel). The lamp and color wheel will be covered for a period of 90 days. The air filter is not covered under warranty.
  - Intelli-M® eIDC controllers
- One year:
  - Video cassette recorders (VCRs), except video heads. Video heads will be covered for a period of six months.
- Six months:
  - All pan and tilts, scanners, or preset lenses used in continuous motion applications (preset scan, tour, and auto scan modes).

Pelco will warrant all replacement parts and repairs for 90 days from the date of Pelco shipment. All goods requiring warranty repair shall be sent freight prepaid to a Pelco designated location. Repairs made necessary by reason of misuse, alteration, normal wear, or accident are not covered under this warranty.

Pelco assumes no risk and shall be subject to no liability for damages or loss resulting from the specific use or application made of the Products. Pelco's liability for any claim, whether based on breach of contract, negligence, infringement of any rights of any party or product liability, relating to the Products shall not exceed the price paid by the Dealer to Pelco for such Products. In no event will Pelco be liable for any special, incidental, or consequential damages (including loss of use, loss of profit, and claims of third parties) however caused, whether by the negligence of Pelco or otherwise.

The above warranty provides the Dealer with specific legal rights. The Dealer may also have additional rights, which are subject to variation from state to state.

If a warranty repair is required, the Dealer must contact Pelco at (800) 289-9100 or (559) 292-1981 to obtain a Repair Authorization number (RA), and provide the following information:

1. Model and serial number
2. Date of shipment, P.O. number, sales order number, or Pelco invoice number
3. Details of the defect or problem

If there is a dispute regarding the warranty of a product that does not fall under the warranty conditions stated above, please include a written explanation with the product when returned.

Method of return shipment shall be the same or equal to the method by which the item was received by Pelco.

RETURNS

To expedite parts returned for repair or credit, please call Pelco at (800) 289-9100 or (559) 292-1981 to obtain an authorization number (CA number if returned for credit, and RA number if returned for repair) and designated return location.

All merchandise returned for credit may be subject to a 20 percent restocking and refurbishing charge.

Goods returned for repair or credit should be clearly identified with the assigned CA or RA number and freight should be prepaid.

12-23-08

Green The materials used in the manufacture of this document and its components are compliant to the requirements of Directive 2002/95/EC.

This equipment contains electrical or electronic components that must be recycled properly to comply with Directive 2002/96/EC of the European Union regarding the disposal of waste electrical and electronic equipment (WEEE). Contact your local dealer for procedures for recycling this equipment.

REVISION HISTORY

Manual #	Date	Comments
C2641M	9/06	Original manual.
C2641M-A	9/07	Added section about changing the Windows XP Embedded administrator password, revised the DX8100 security information, antivirus section, and updated system recovery procedure for Windows XP Embedded.
C2641M-B	4/08	Added a section about how to use a network management system to communicate with the DX8100.
C2641M-C	7/09	Added the safe mode section, removed the Windows 2000 and upgrade and recovery sections.

Pelco, the Pelco logo, Camclosure, Digital Sentry, Endura, Esprit, ExSite, Genex, Intelli-M, Legacy, and Spectra are registered trademarks of Pelco, Inc.
Spectra III is a trademark of Pelco, Inc.
DLP is a registered trademark of Texas Instruments Incorporated.
All product names and services identified throughout this document are trademarks or registered trademarks of their respective companies.
The absence of a trademark or registered trademark from this document does not constitute a waiver of intellectual property rights.

© Copyright 2009, Pelco, Inc. All rights reserved.

www.pelco.com

Pelco, Inc. Worldwide Headquarters 3500 Pelco Way Clovis, California 93612 USA
USA & Canada Tel (800) 289-9100 Fax (800) 289-9150
International Tel +1 (559) 292-1981 Fax +1 (559) 348-1120